

III. AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Previously Presented) A computerized method for protecting an identifier of a subscriber, during data transfer between a service provider and a content provider, when said subscriber sends a request to said service provider to obtain data belonging to said content provider, said computerized method comprising:

executing on at least one computer the steps including:

upon reception of said subscriber request by said service provider for each new subscriber session:

dynamically generating for each new session an encrypted token using said identifier of said subscriber, wherein a lifetime of the encrypted token is a user session lifetime, the generating using one of a symmetric and asymmetric encryption algorithm comprising:

determining a separator (S);

determining a time varying value (T);

concatenating the subscriber identifier with T in a string such that the subscriber identifier and T are separated with S;

encrypting the string with one of a symmetric and asymmetric encryption algorithm; and,

transmitting said subscriber request and said encrypted token to said content provider;

upon reception by said service provider of a Simple Object Access Protocol (SOAP) certification request comprising an encrypted token, sent by said content provider:

extracting said encrypted token from said SOAP certification request, wherein the encrypted token is in one of the SOAP body and a predefined SOAP header;

decrypting said extracted encrypted token using a decryption algorithm corresponding to the encryption algorithm;

retrieving the subscriber identifier using the separator;

checking said determined subscriber identifier; and,

transmitting a success or failure indication to said content provider in a SOAP response to said certification request;

upon reception of said data belonging to said content provider by said service provider, transmitting said data belonging to said content provider to said subscriber; and

memorizing said encrypted token so that it can be reused during the user session lifetime without having to be recomputed; and

formatting said data belonging to said content provider in a format suitable and usable by the subscriber.

2. (Original) The method of claim 1, further comprising the step of verifying rights of said subscriber, wherein said steps of computing an encrypted token and transmitting said subscriber request and said encrypted token to said content provider are done only

if said subscriber holds corresponding rights.

3. (Canceled)

4. (Original) The method of claim 1 further comprising the step of charging said subscriber if said determined subscriber identifier is certified.

5. (Canceled)

6. (Canceled)

7. (Canceled)

8. (Original) The method of claim 1 implemented using web service technology.

9. – 10 (Canceled)